(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－90157
（P2000－90157A）
(43)公開日　平成12年３月31日(2000.3.31)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　17/60		Ｃ０６Ｆ　15/21	Ｚ	５Ｂ０４９

審査請求　未請求　請求項の数３　ＯＬ　（全　８　頁）

(21)出願番号　特願平10－261828

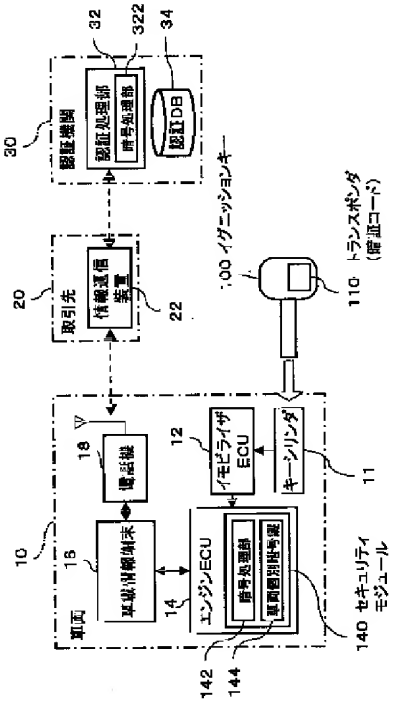
(22)出願日　平成10年９月16日(1998.9.16)

(71)出願人　000003207
トヨタ自動車株式会社
愛知県豊田市トヨタ町１番地
(72)発明者　平松　紀昌
愛知県豊田市トヨタ町１番地　トヨタ自動車株式会社内
(74)代理人　100075258
弁理士　吉田　研二　（外２名）

Ｆターム(参考)　5B049 AA01 AA05 BB11 CC05 CC39 CC40 EE23 GG06 GG10

(54)【発明の名称】　移動体用認証システム

(57)【要約】
【課題】　車両等からの購入要求等の認証の際の利用者の操作負担を軽減する。
【解決手段】　車載情報端末１６は、購入要求等の生成に当たり、テストデータをセキュリティモジュール１４０に渡す。正しいイグニッションキー１００が使われている場合、モジュール１４０は、そのキーの暗証コードをイモビライザＥＣＵ１２から取得し、これを用いてテストデータを暗号化する。端末１６はこの暗号化結果を認証情報として取引先２０に送る。取引先２０は、認証情報を認証機関３０に渡す。認証機関３０は、認証ＤＢ３４に予め登録された当該車両利用者の暗証コードを検索し、これを用いて認証情報を復号化し、復号化結果がテストデータと一致すれば、正当な利用者である旨の認証結果を取引先２０に返す。取引先２０はこの認証結果を受けて購入要求を承認する。盗難防止のためのイモビライザの暗証コードを認証に利用することにより、クレジットカード番号の入力操作等が不要になる。



【特許請求の範囲】
【請求項１】　駆動手段始動指令を受けたときにイグニッションキーが有する暗証コードを検出し、その検出結果に応じて該駆動手段の始動の許可・不許可を決定する盗難防止手段を有する移動体と、前記移動体からの通信アクセスに関する認証を行う認証機関と、を含む移動体用認証システムであって、
前記移動体は、
前記盗難防止手段からイグニッションキーの暗証コードを取得し、この暗証コードを鍵として所定のテストデータを暗号化することにより認証情報を生成する認証情報生成手段と、
前記認証情報生成手段で生成された認証情報を前記移動体の利用者の識別データに対応づけて発行する手段と、を有し、
前記認証機関は、
各イグニッションキーごとに、該キーの暗証コードに対応する参照コードと、該キーに対応づけられた利用者の識別データと、を対応づけて記憶する認証データベースと、
移動体が発行した利用者識別データ及び認証情報を受け取り、この識別データに対応する参照コードを前記認証データベースから検索し、検索した参照コードとその認証情報とに基づき、その認証情報の生成に用いられた暗証コードが正当なものであるかを判定し、この判定結果に応じて前記認証情報に対応する通信アクセスに関する認証を行う認証手段と、
を有する移動体用認証システム。
【請求項２】　請求項１記載のシステムであって、
前記移動体の前記認証情報生成手段は、前記認証情報の生成に当たり、該移動体自体に割り当てられた個別鍵情報を、前記イグニッションキーの暗証コードとともに用いて暗号化を行い、
前記認証機関の前記認証データベースは、各イグニッションキーごとに、該キーに対応する移動体に割り当てられた個別鍵情報に対応する参照鍵情報を更に記憶し、
前記認証機関の前記認証手段は、受け取った識別データに対応する参照コード及び参照鍵情報を前記認証データベースから検索し、この検索結果と該識別データに対応して受け取った認証情報とに基づき、該認証情報の生成に用いられた暗証コード及び個別鍵情報が正当なものであるかを判定し、この判定結果に応じて認証を行うことを特徴とする移動体用認証システム。
【請求項３】　請求項１又は請求項２に記載のシステムであって、
前記認証データベースは、各イグニッションキーごとに、当該キーに対応づけられた利用者のクレジット情報を更に記憶し、
前記認証手段は、前記移動体が発行した認証情報が正当な鍵により暗号化されたものであると判定した場合には、前記移動体から受け取った識別データに対応するクレジット情報についての決済を可能とすることを特徴とする移動体用認証システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、車両等の移動体からの通信アクセスに関する利用者認証に関する。
【０００２】
【従来の技術】社会の高度情報化の進展に伴い、自動車に高機能の情報通信装置を搭載し、運転者等に通信ネットワークを介して種々の情報やサービスを提供することが可能となっている。例えば、自動車に対する交通情報等の情報提供サービスや電子メールサービスなどは既に実現されている。
【０００３】ネットワークを利用したサービスの一つに、オンラインショッピングがある。オンラインショッピングでは、ネットワークを介した代金の決済（電子決済）をいかに行うかが一つの課題である。このような電子決済の方法として、電子マネー方式やクレジットカード方式など種々の方式が提案され、実用化されている。
【０００４】クレジットカード方式の電子決済において問題となるのが、本人認証である。従来、例えばインターネット等のオンラインショッピングでの電子決済では、最も単純には、ユーザにクレジットカード番号を入力させることで本人認証を行っていた。また、もっとセキュリティを向上させた方法として、暗号処理機能を搭載したＩＣカードをクレジットカードとして用い、このカードをカードリーダに挿入し、ホストとの間で暗号を利用して認証を行う方法も知られている。
【０００５】
【発明が解決しようとする課題】クレジットカード番号入力やＩＣカード利用の方法は、パーソナルコンピュータや専用のカード端末をベースとしており、番号入力のための手段やカードリーダなどを必要とする。
【０００６】ところが、現状の自動車に搭載される情報通信装置は、スペース的な制限などからクレジットカード番号の入力手段（例えばキーボード）やカードリーダなどが装備されておらず、上記方法をそのまま適用することは困難である。また、仮にそのような手段を設けたとしても、自動車では、他の装置との関係や安全面の配慮からそのような手段を配置できる場所が限られており、パソコンや専用端末に比べて操作が面倒になりがちである。自動車での利用を考えた場合、利用者（運転者等）にあまり負担をかけずに認証情報を取り込むことができる仕組みが望まれる。
【０００７】以上、自動車からの電子決済の場合を例にとったが、自動車等の移動体から通信によりサービスを受けるケースはこの他にも様々あり、上記同様認証が必要となるケースも多い。上記課題は、このようなケースにも共通するものである。

【０００８】本発明はこのような課題に鑑みなされたものであり、自動車等の移動体からの通信アクセスについての認証において、運転者等の利用者に負担をかけずに認証情報を取り込むことができるシステムを提供することを目的とする。

【０００９】

【課題を解決するための手段】上記課題を解決するため、本発明では、移動体に設けられている盗難防止手段の暗証コードを、認証のための基本データとして利用する。ここでいう盗難防止手段は、イグニッションキーに暗証コードを組み込み、このキーによるエンジン（駆動力源のことでありモーターなども含む）始動操作の際にその暗証コードを検査して始動の可否を制御するというものであり、これはイモビライザ（Imobilizer）として公知の技術である。移動体から認証を求める場合、この盗難防止手段から暗証コードを用いて所定の情報を暗号化し、この暗号化結果を識別データに対応づけて認証情報として発行する。認証機関には各イグニッションキーごとに、そのキーの暗証コードに対応する参照コードとそれに対応する利用者の識別データが登録されている。ここで、暗証コードが認証情報作成時の鍵として用いられたのに対し、参照コードはその認証情報の検証のための鍵である。例えば、本システムの暗号方式として秘密鍵暗号系を用いた場合、参照コードは暗証コードと全く同じものであり、公開鍵暗号系を用いた場合、参照コードは暗証コードに対応する公開鍵である。認証機関は、認証を受けようとする利用者の識別データに対応づけられた認証情報を受け取り、その識別データに対応する参照コードを用いて認証情報を検証する。例えば、認証情報を参照コードで復号化したときに、その復号化結果が認証情報の元となった所定の情報と一致すれば、認証を受けようとする利用者が正当であると判定できる。この構成によれば、認証を受けるに当たって、移動体内の利用者がクレジットカード番号の入力やＩＣカードの挿入などといった操作を行う必要がなく、操作負担が軽減される。

【００１０】また、この発明において、認証データベースに登録した参照鍵情報を移動体自体に個別鍵情報として付与し、認証情報の生成に当たりこの個別鍵情報も暗号化鍵として用いることにより、認証機関にて、イグニッションキーの正当性だけでなく、移動体自体の正当性も検証できる。

【００１１】また、この発明において、認証データベースに利用者のクレジット情報を登録するようにすれば、移動体にてクレジット情報の入力等の操作を行うことなく、クレジットカードによる決済を受けることが可能になる。

【００１２】

【発明の実施の形態】以下、本発明の実施の形態（以下実施形態という）について、図面に基づいて説明する。

【００１３】［実施形態１］図１は、本発明に係る第１の実施形態のシステム構成の一例を示す図である。図１は、オンラインショッピング等の電子商取引における電子決済のためのシステム構成例であり、通信ネットワークを介して取引を行う車両１０と取引先２０に加え、該車両１０の取引先２０への購入要求について認証を与える認証機関３０を含んでいる。

【００１４】車両１０は、搭乗者に対してナビゲーションサービスや各種情報処理・通信サービスを提供する車載情報端末１６を有している。車載情報端末１６は、自動車電話や携帯電話等の電話機１８を介して、インターネットや商用ネットワークに接続できる。また、車両１０は、車両用の盗難防止機構の一つであるイモビライザ（Imobilizer）システムを搭載している。イモビライザシステムは、キーシリンダ１１、イモビライザＥＣＵ（electronic control unit）１２及びエンジンＥＣＵ１４により実現されている。本実施形態では、このイモビライザの情報を利用し、車両１０の購入要求についての認証を実現する。

【００１５】イモビライザについては、例えば自動車技術事例集／発行番号９５６０３（日本自動車工業会知的財産部会１９９５．１２．１発行）に説明があるので、ここでは図面に即し、本発明に関連する部分を主に、その概略を説明する。

【００１６】イモビライザシステムでは、イグニッションキー１００に暗証コード送信用のトランスポンダ１１０を内蔵する。トランスポンダ１１０は、車両１０のキーシリンダ１１に設けられたアンテナからの電波から電力をもらい、記憶している暗証コードを送信する。キーシリンダ１１のアンテナは、イモビライザＥＣＵ（electronic control unit）１２に接続されており、イグニッションキー１００から受信した暗証コードをイモビライザＥＣＵ１２に渡す。イモビライザＥＣＵ１２は、正しいイグニッションキーの暗証コードに関する情報を有しており、イグニッションキー１００から送られてきた暗証コードが正しいものか否かを判定する。この判定結果は、エンジンの点火（イグニッション）及び燃料供給（フューエルインジェクション）を制御するエンジンＥＣＵ１４に送られる。イモビライザＥＣＵ１２で正しい暗証コードが得られなかった場合は、エンジンＥＣＵ１４がエンジンへの燃料供給及びエンジン点火を禁止し、エンジンを停止制御する。したがって、正しいイグニッションキーを使用せずに始動しようとした場合には、以上の仕組みによりエンジンの始動及び車両の走行が防止される。

【００１７】イグニッションキー１００は、１台の車両に対して複数個発行することができる。この場合、同じ車両に対するものであっても、各イグニッションキー１００にはそれぞれ異なる暗証コードを付与する。そして、イモビライザＥＣＵ１２には、当該車両１０に割り

当てられた各イグニッションキー１００の正しい暗証コードの情報が登録される。これにより、車両１０の正しいイグニッションキー１００であれば、どれを用いても正しくエンジンを始動させることができる。

【００１８】本実施形態では、このイモビライザシステムにおけるイグニッションキー１００の暗証コードを、車両１０からの購入要求に対する認証のための基礎情報として利用する。

【００１９】このため、本実施形態では、車両１０に、認証情報を生成するためのセキュリティモジュール１４０を設ける。セキュリティモジュール１４０は、イモビライザＥＣＵ１２からイグニッションキー１００の暗証コードを受け取り、これに基づき認証情報を生成する。図１の例では、セキュリティモジュール１４０は、イモビライザＥＣＵ１２に接続されたエンジンＥＣＵ１４内に設けられているが、セキュリティモジュール１４０をエンジンＥＣＵ１４とは別体のＥＣＵとして構成してももちろんよい。

【００２０】セキュリティモジュール１４０は、暗号処理部１４２を有すると共に、車両個別暗号鍵１４４を記憶している。車両個別暗号鍵１４４は、イグニッションキー１００の暗証コードとは別に、車両１０そのものに対して付与された暗号化鍵である。すなわち、イグニッションキーの暗証コードは１台の車両に対し複数個対応づけられる可能性がある（すなわちキーが複数個発行された場合）が、車両個別暗号鍵１４４は１台の車両に対し１個付与されるだけである。暗号処理部１４２は、イモビライザＥＣＵ１２から与えられるイグニッションキー１００の暗証コードとセキュリティモジュール１４０の車両個別暗号鍵１４４の２つのデータを鍵データとして用い、車載情報端末１６から与えられる情報を暗号化する。この暗号化結果が、本システムにおける認証情報となる。この認証情報は、ネットワークを介した商取引のためのプロトコルに従い、購入要求に対応づけて取引先２０に送られる。

【００２１】取引先２０は、ネットワークを介した取引処理を実行する情報通信装置２２を有する。情報通信装置２２は、ネットワークを介して車両１０から購入要求を受け取り、この購入要求に付随して受け取った認証情報を認証機関３０に送って、その認証を依頼する。

【００２２】認証機関３０は、認証のための情報を登録した認証データベース（ＤＢ）３４と、認証処理を行う認証処理部３２を有している。

【００２３】認証ＤＢ３４の有するデータ内容の一例を図２に示す。認証データベース３４には、各利用者の利用者ＩＤに対応づけて、当該利用者の車両の車両個別暗号鍵、この車両のイグニッションキーのうち当該利用者に付与されたキーの暗証コード、当該利用者のクレジット情報（カード番号など）が登録される。利用者ＩＤは、ネットワークにおける当該利用者の識別情報であり、インターネットであれば電子メールアドレス、商用ネットワークであればネットワークホストから当該利用者に付与されたＩＤ番号などを用いることができる。

【００２４】車両個別暗号鍵は、認証機関３０により付与され、車両製造時に車両メーカーによりエンジンＥＣＵ１４内に設定される。イグニッションキーの暗証コードは、車両メーカーによって各キーごとに一意な値として付与され、イグニッションキーに組み込まれる。この暗証コードは、車両メーカーと認証機関との取り決めに従って認証機関に通知され、対応する車両の車両個別暗号鍵と対応づけて認証ＤＢ３４に登録される。認証機関３０は、利用者の車両購入時あるいは利用者から要求があったとき等に、当該利用者からネットワークの利用者ＩＤ及びクレジット情報の通知を受け、これらを当該車両の車両個別暗号鍵及び当該利用者に割り当てられたイグニッションキー暗証コードに対応づけて認証ＤＢ３４に登録する。

【００２５】認証機関３０の認証処理部３２は、この認証ＤＢ３４の登録情報に基づき、取引先２０から依頼された認証処理を行う。認証処理部３２は、車両１０のセキュリティモジュール１４０に組み込まれた暗号処理部１４２と同じ暗号アルゴリズムで暗号処理を行う暗号処理部３２２を有する。認証処理部３２は、取引先２０からの認証依頼に付随して送られてくる車両１０の認証情報を、暗号処理部３２２で復号化し、その正当性を検査する。そして、認証情報が正当なものと判定された場合は、認証処理部３２は、依頼元の取引先２０に対し、依頼に係る購入要求についての認証を与え、その購入要求元の利用者のクレジット情報を通知する。なお、この認証処理の詳細な手順については後にあらためて説明する。

【００２６】次に、図１のシステム構成例における一連の処理手順を図３を参照して説明する。まず、車両１０に搭乗した利用者が、車載情報端末１６に対して取引先２０の商品等の購入操作を行うと、所定の通信プロトコルに従って両者の間に通信路が設定される。また、車載情報端末１６は、この通信路設定の後又は通信路設定と並行して、所定の方法によりテストデータを生成し、セキュリティモジュール１４０に対し、テストデータを引数として暗号化要求コマンドを発行する。このテストデータは、認証情報の元となるデータであり、認証情報の固定化を防ぐためにはこのテストデータも固定値でない方が望ましい。例えばテストデータを乱数発生により生成することも好適である。

【００２７】このテストデータを引数とした暗号化要求コマンドを受けたセキュリティモジュール１４０では、暗号処理部１４２が、まずイグニッションキー１００の暗証コードを暗号化鍵としてテストデータを暗号化する。ここで、イグニッションキーの暗証コードは、イモビライザＥＣＵ１２から与えられる。すなわち、イモビ

ライザＥＣＵ１２は、キーシリンダ１１が正しいイグニッションキー１００を受け付けている間のみ、そのキーの暗証コードを暗号処理部１４２に供給し、暗号処理部１４２はこの暗証コードを用いて暗号化処理を実行する。

【００２８】次に暗号処理部１４２は、暗証コードによる暗号化結果を、更に車両個別暗号鍵で暗号化する。したがって、テストデータは、イグニッションキーの暗証コードと車両個別暗号鍵とで２重に暗号化されることになる。セキュリティモジュール１４０は、このように２重に暗号化されたテストデータを、認証情報として車載情報端末１６に返す。

【００２９】認証情報を受け取った車載情報端末１６は、購入要求を生成し、通信路を介して取引先２０に送信する。ここで、購入要求は、認証のための情報として、要求を発行した利用者の利用者ＩＤ、セキュリティモジュール１４０から得た認証情報、及びその認証情報の元のテストデータ、を含んだ形で生成される。これらの情報が、購入要求の内容を示す購入内容情報とともに、取引先に送られる。なお、ここで、認証情報及びテストデータは前述の如く車載情報端末１６及びセキュリティモジュール１４０により自動的に生成されるものであり、これらの生成に当たり利用者の操作は全く必要ない。また、利用者ＩＤも、車載情報端末１６の通信アプリケーションプログラムに予め設定されているのが一般的であり、購入要求に当たって改めて入力する必要はない。したがって、利用者は、購入操作を行うだけで他に特別の操作を行わなくても、自動的に認証のための情報が生成され、送信されることになる。

【００３０】購入要求を受け取った取引先２０は、認証機関３０との間に通信路を設定し、購入要求に含まれる認証のための情報、すなわち利用者ＩＤ、認証情報、及びテストデータを認証機関３０に送り、認証を依頼する。

【００３１】認証依頼を受けた認証機関３０では、認証処理部３２により図４に示す手順で認証が行われる。まず認証処理部３２は、認証依頼に含まれる利用者ＩＤをキーとして認証ＤＢ３２を検索し、その利用者ＩＤに対応するイグニッションキーの暗証コードと車両個別暗号鍵を取得する（Ｓ１００）。次に、暗号処理部３２２にて、認証依頼に含まれる認証情報を、検索した暗証コード及び車両個別暗号鍵を用いて復号化する（Ｓ１０２）。そして、認証処理部３２は、この復号化結果を、認証依頼に含まれるテストデータと比較する（Ｓ１０４）。なお、本実施形態では暗号方式として秘密鍵方式を用いているので、この処理手順で認証機関側が認証のために用いる鍵は、車両側で暗号化に用いた鍵（すなわち暗証コード及び車両個別暗号鍵）と結果的に同じものになる。しかしながら、両者は概念的には異なったものであり、認証機関側で用いる暗証コード及び車両個別暗号鍵は、特許請求の範囲における参照コード及び参照鍵情報にそれぞれ対応する。

【００３２】利用者が自分の利用者ＩＤに対応する正しいイグニッションキー（暗証コード）を用いて、正しい車両から購入要求を発した場合は、復号化結果とテストデータとは一致するはずである。したがって、両者が一致しなかった場合（Ｓ１０６の判定結果が否定（Ｎｏ））は、認証処理部３２は、該認証依頼に係る通信アクセスが不正（ＮＧ）であると判断し、その旨を示す認証結果を取引先２０に返す（Ｓ１０８）。一方、復号化結果とテストデータとが一致した場合は、該認証依頼に係る通信アクセスが正当（ＯＫ）であると判断し、認証ＤＢ３４から当該利用者ＩＤに対応するクレジット情報を検索する（Ｓ１１０）。そして、検索したクレジット情報を含む認証結果（ＯＫ）を生成し、取引先２０に返信する（Ｓ１１２）。

【００３３】なお、図４の例では、認証情報の復号結果とテストデータとを比較して正当性の判定を行ったが、正当性の判定方法はこれに限らない。テストデータの暗号化結果である認証情報が正しい暗号化鍵（暗証コード及び車両個別暗号鍵）によって暗号化されたものであることが検査できる方法であれば、いかなる方法でも良い。例えば、テストデータを暗証コード及び車両個別暗号鍵で暗号化した結果を認証情報と比較する方法でもよい。

【００３４】認証機関３０から認証結果を得た取引先２０は、その認証結果がＮＧの場合は、車両１０からの購入要求を拒否し、その旨を示す購入応答を車両１０に返す。一方、認証結果がＯＫの場合は、その認証結果に付随して送られてきたクレジット情報を用いてさらにクレジットカード会社等に信用照会を行い、この照会結果に応じて車両１０からの購入要求の承認・拒否を決定し、その結果を示す購入応答を車両１０に返す。そして、購入要求を承認した場合は、そのクレジット情報を用いて購入代金の決済処理を実行する。

【００３５】以上、車両からのオンラインショッピングの電子決済処理の場合を例として、本発明の好適な実施形態を説明した。本実施形態では、車両に搭載されている盗難防止機構の暗証コードを認証に利用することにより、クレジットカード番号等の入力やＩＣカードの挿入がなくても認証を行うことができるので、車載情報端末に番号入力手段やＩＣカードリーダなどの特別の入力手段を設ける必要がない。また、利用者による認証情報の入力操作も必要ないので、利用者の操作負担も軽減される。このメリットは、利用者の位置や姿勢が制限される車両等においては大きな意味を持つ。また、本実施形態では、電子決済に当たり、クレジット情報を車両から取引先に送る必要がなくなるので、クレジット情報漏洩のリスクを軽減することができる。

【００３６】また、本実施形態では、イグニッションキ

ーの暗証コードと、車両に組み込まれた車両個別暗号鍵及び暗号化アルゴリズムとがすべて正しくないと正当性が認証されないので、非常に強いセキュリティ効果を得ることができる。例えば、何者かが何らかの手段でイグニッションキー又はその暗証コードを入手したとしても、それだけでは当該キーの持ち主になりすますことはできない。

【００３７】また、本実施形態では、車両側の暗号処理機構をセキュリティモジュール１４０として車両１０本体に組み込むようにした。この構成において、車載情報端末１６の通信アプリケーションとセキュリティーモジュール１４０との間のインタフェースを暗号化要求コマンドとそれに対する認証情報の応答に限定するように構成すれば、暗号化アルゴリズムや車両個別暗号鍵等に対し、車載情報端末１６のユーザインタフェースから直接アクセスすることができなくなる。したがって、暗号処理機構を車載情報端末１６にソフトウエアとして組み込む場合より暗号アルゴリズムや車両個別暗号鍵の窃取が困難になり、安全性がより高まる。

【００３８】また、本実施形態では、１車両に複数のイグニッションキーを発行した場合、各キーごとに決済の可否や決済先を設定することもできる。すなわち、認証ＤＢにキーに対応するクレジット情報を登録しなければそのキーを用いても決済は不可能であり、ま各キーに対応づけるクレジット情報を各キーごとに変えると、別のキーを用いれば別のカードで決済されることになる。

【００３９】なお、本実施形態には、本発明の範囲内で様々な変形が考えられる。例えば、上記の例では、イグニッションキーの暗証コード及び車両個別暗号鍵の２つの鍵でテストデータを暗号化するに当たり、それら２つの鍵を順に適用して二重の暗号化を行ったが、これは必須ではない。暗証コードと車両個別暗号鍵の両方が正当であることが検証できるような暗号化方式であれば、どのような方式でも適用可能である。例えば、２つの鍵をつなげたものを鍵として１回だけ暗号化を行うような方式も考えられる。また、認証機関３０から取引先２０に利用者のクレジット情報を送るに当たり、クレジット会社の暗号鍵によりクレジット情報を暗号化して送るようにすることにより、取引先２０に対して利用者の秘密を守りつつ、クレジット処理を行うこともできる。

【００４０】［実施形態２］図５を参照して、本発明の別の実施形態について説明する。上記実施形態１は電子商取引の例であったが、実施形態２は車両情報のダウンロードの場合の認証手順の例を示す。

【００４１】車両を対象としたネットワーク情報サービスとして、個々の車両あるいは運転者に固有の情報をネットワークホスト側で作成し、これを運転者等からの要求に応じて提供するというサービスが考えられる。このようなサービスでは、プライバシー保護の観点から、車両からの情報要求が正当なものであるかをホスト側で検査（認証）する必要がある。この検査に、本発明に係る認証方式を適用することができる。

【００４２】この実施形態では、情報提供を行うホスト４０が認証機関の機能（すなわち、図１の認証処理部３２及び認証ＤＢ３４）を有する。ただし、認証ＤＢにはクレジット情報を登録する必要がなく、またこの実施形態では車両個別暗号鍵を用いないのでその登録も必要ない。車両１０側の認証処理のための機能構成は、図１の構成と同様でよい。ただし、セキュリティモジュール１４０に車両個別暗号鍵を組み込む必要はない。

【００４３】図５の手順において、車両１０の車載情報端末１６に対し、利用者が情報要求操作を行うと、車載情報端末１６は利用者ＩＤと要求内容を含んだ情報要求を生成し、ホスト４０に対して送信する。これを受けたホスト４０は、要求された情報が予め定められた秘密保護対象であるかを判定し、秘密保護対象であるばあいには、所定の認証処理を行う。認証処理においては、ホスト４０は、まず乱数発生などの手段でテストデータを生成し、このテストデータを引数とする認証情報要求を車載情報端末１６に対して返す。車載情報端末１６は、そのテストデータをセキュリティモジュール１４０に渡して暗号化要求を行う。これを受けたセキュリティモジュール１４０は、実施形態１と同様イモビライザＥＣＵ１２からイグニッションキーの暗証コードを取得し、この暗証コードでテストデータを暗号化し、この暗号化結果を認証情報として車載情報端末１６に返す。これを受けた車載情報端末１６は、この認証情報を、認証情報要求に対する応答としてホスト４０に返す。

【００４４】ホスト４０は、利用者ＩＤに対応する暗証コードを認証ＤＢから検索し、車両１０から返信されてきた認証情報を、検索した暗証コードを用いて復号化する。そして、ホスト４０は、前に車両１０に渡したテストデータとその復号化結果とを比較し、両者が一致した場合は正当な利用者からの情報要求と判断し、要求された情報をその車両１０に返信する。一方、復号化結果がテストデータと一致しなかった場合は、不正な要求と判断し、情報要求を拒否する旨の通知を車両１０に返す。

【００４５】このように、本実施形態によれば、利用者が正しい車両にて正しいイグニッションキーを用いている場合にのみ、ホストからその車両に情報提供がなされる。この認証方式は、車載情報端末１６のオペレーティングシステムやアプリケーション等のソフトウエアのダウンロードやバージョンアップにも好適である。すなわち、この認証方式によれば、家庭のパーソナルコンピュータなど、車載情報端末以外のコンピュータからのダウンロード等を防ぐことができ、車載情報端末用ソフトウエアの不正コピー等の防止に効果がある。

【００４６】以上、本発明の各実施形態について説明した。以上の各実施形態ではテストデータとして乱数を用いたので、認証のために、車両側から認証機関側にテス

トデータを送るか（実施形態１）、認証機関側でテストデータを生成して車両側に送るか（実施形態２）の対応をとっていた。これに対し、テストデータの生成方式を車両と認証機関との間で取り決めておき、どちらでも同じテストデータを得られるようにしておけば、車両と認証機関との間でテストデータを受け渡す必要がなくなる。この方式の最も単純な例としては、日付情報をテストデータとする方法があげられる。

【００４７】また、上記各実施形態では、認証情報の生成のための暗号化方式として、車両と認証機関との間で同じ暗号鍵（すなわち暗証コード、車両個別暗号鍵）を共有する秘密鍵方式（共有鍵方式とも呼ばれる）の暗号化方式を用いたが、これは本発明にとって必須のことではない。公開鍵方式を用いて上記実施形態と同様のシステムを構成することももちろん可能である。公開鍵方式の場合は、イグニッションキーの暗証コードや車両個別暗号鍵そのものでなく、それらから生成した公開鍵を認証ＤＢに登録すればよく、認証は公開鍵方式における電子署名の方法を利用して行うことができる。

【００４８】また、以上の各実施形態で示した認証処理の手順は例示的なものであり、イグニッションキーの暗証コードを認証のための情報として利用するという技術的思想は、各実施形態にしめした以外の認証処理手順にも適用可能である。

【００４９】また、車両に対する情報サービスを行うネットワークにおいては、利用者ではなく車両自体に識別番号を付与して管理する場合も考えられるが、このような場合、イグニッションキーの暗証コードやクレジット情報などの認証のための情報は、車両の識別番号に対応づけて認証ＤＢに登録すればよい。この場合の車両の識別番号は利用者ＩＤの一種であり、上記各実施形態と全く同じ扱いで認証処理を実現できる。

【００５０】また、上記各実施形態の方法にパスワード認証処理を併用することも好適である。すなわち、認証ＤＢにおいて、イグニッションキーに対応づけてパスワードを登録しておき、購入要求等においてパスワード入力を求めるようにすれば、安全性をより高めることができる。

【００５１】また、以上の実施形態は車両についてのものであったが、本発明の方式は、イモビライザと同様のシステムを有するものであれば、船舶、航空機その他の移動体にも当然適用可能である。また、本発明に係る認証処理の適用分野が、例示した電子決済やダウンロード可否判定の場合に限られないことも明らかであろう。

【図面の簡単な説明】

【図１】　本発明に係るシステムの構成を示す図である。

【図２】　認証ＤＢ（データベース）の登録データ内容の一例を示す図である。

【図３】　実施形態１における認証処理の手順を示す図である。

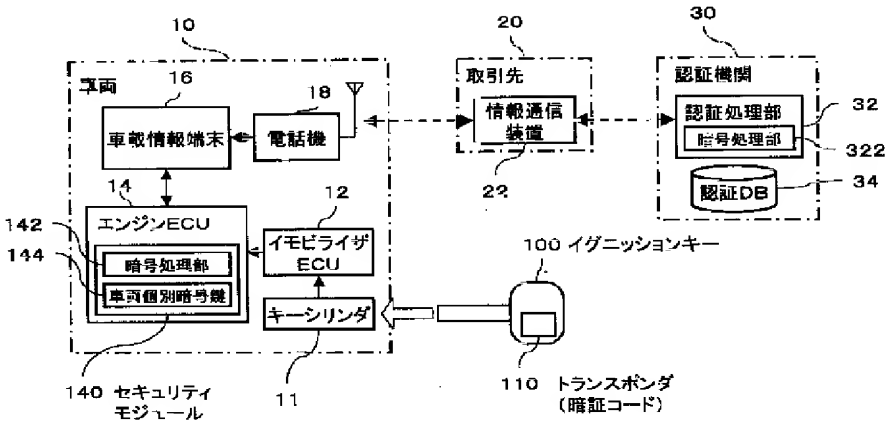
【図４】　認証機関による認証処理の手順を示すフローチャートである。

【図５】　実施形態２における認証処理の手順を示す図である。

【符号の説明】

１０　車両、１１　キーシリンダ、１２　イモビライザＥＣＵ、１４　エンジンＥＣＵ、１６　車載情報端末、１８　電話機、２０　取引先、２２　情報通信装置、３０　認証機関、３２　認証処理部、３４　認証ＤＢ（データベース）、１００　イグニッションキー、１１０　トランスポンダ、１４０　セキュリティモジュール、１４２，３２２　暗号処理部、１４４　車両個別暗号鍵。

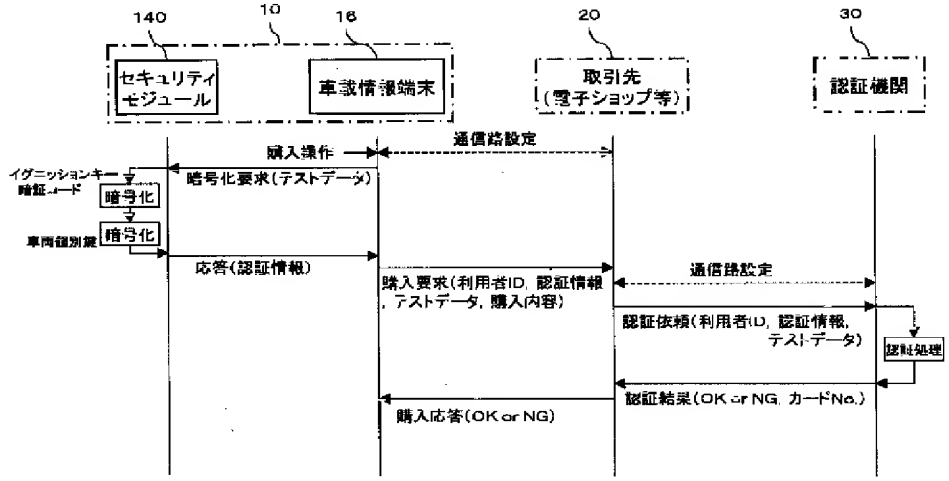
【図１】



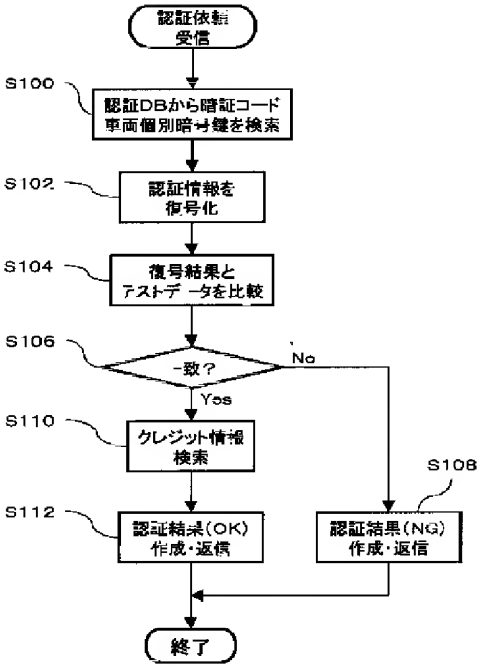
【図2】

利用者ID	イグニッションキー暗証コード	車両個別暗号鍵	クレジット情報
12345678	xxxxxxxxx	oooooooo	△△△△△△
23456789	**********	##########	□□□□□□
・	・	・	・
・	・	・	・
・	・	・	・

【図3】



【図4】



【図5】